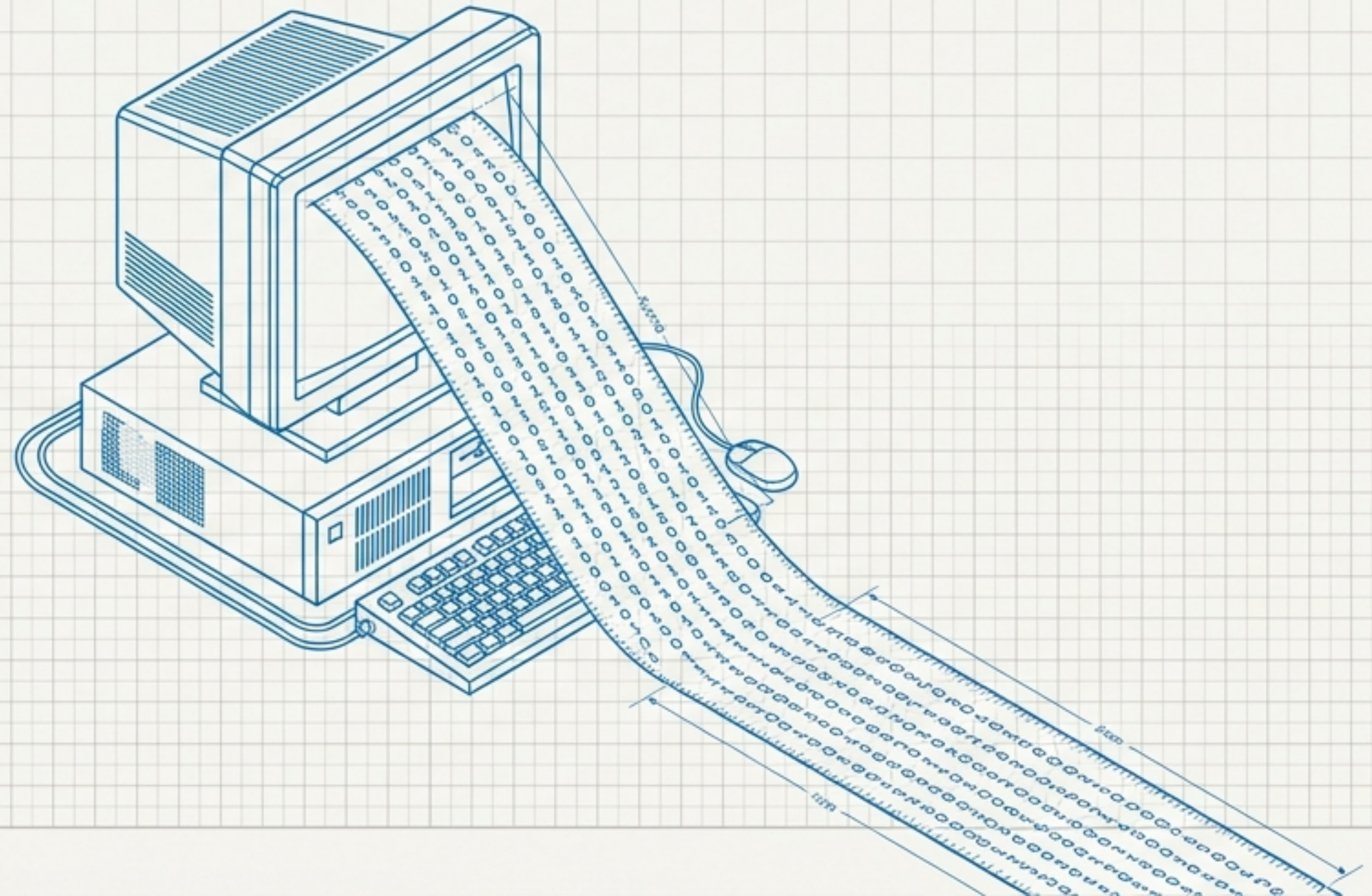


Analyse Forensique des Terminaux : L'Architecture de la Preuve

Méthodologies de pointe pour l'investigation numérique, l'analyse des systèmes de fichiers et la récupération de données.



« L'homme reste l'ordinateur
le plus extraordinaire qui soit. »
—John F. Kennedy

**15
Milliards**
(Aujourd'hui)

**50
Milliards**
(2020)

**500
Milliards**
(2030)

Le Défi (Volume écrasant)

La prolifération de l'Internet des Objets (IoT) complexifie l'acquisition, multipliant les terminaux à analyser (ordinateurs, serveurs, IoT).

L'Opportunité (Mines de preuves)

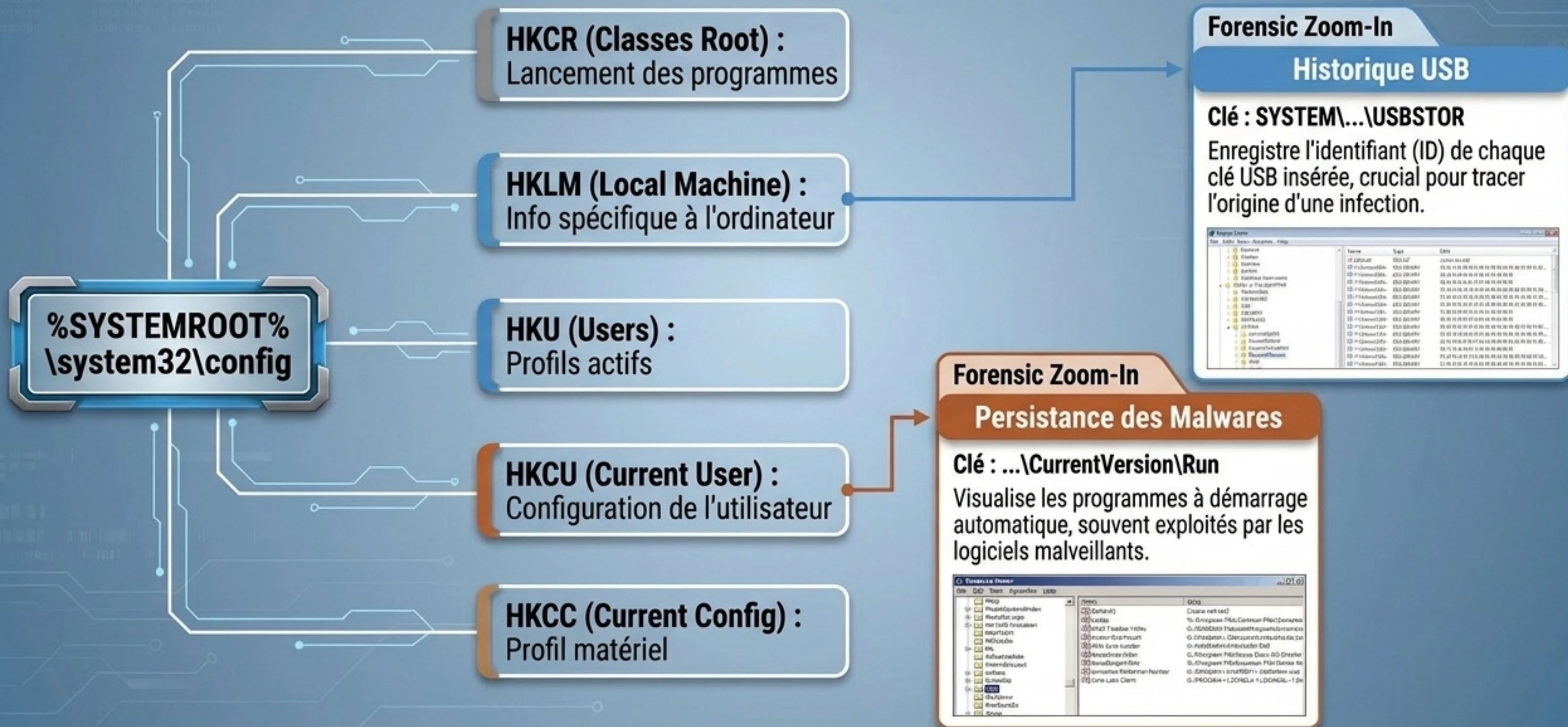
Ces appareils enregistrent continuellement des aspects de la vie quotidienne, créant une empreinte numérique indélébile, cruciale pour les enquêtes ultérieures.

Les Fondations : Systèmes de Fichiers

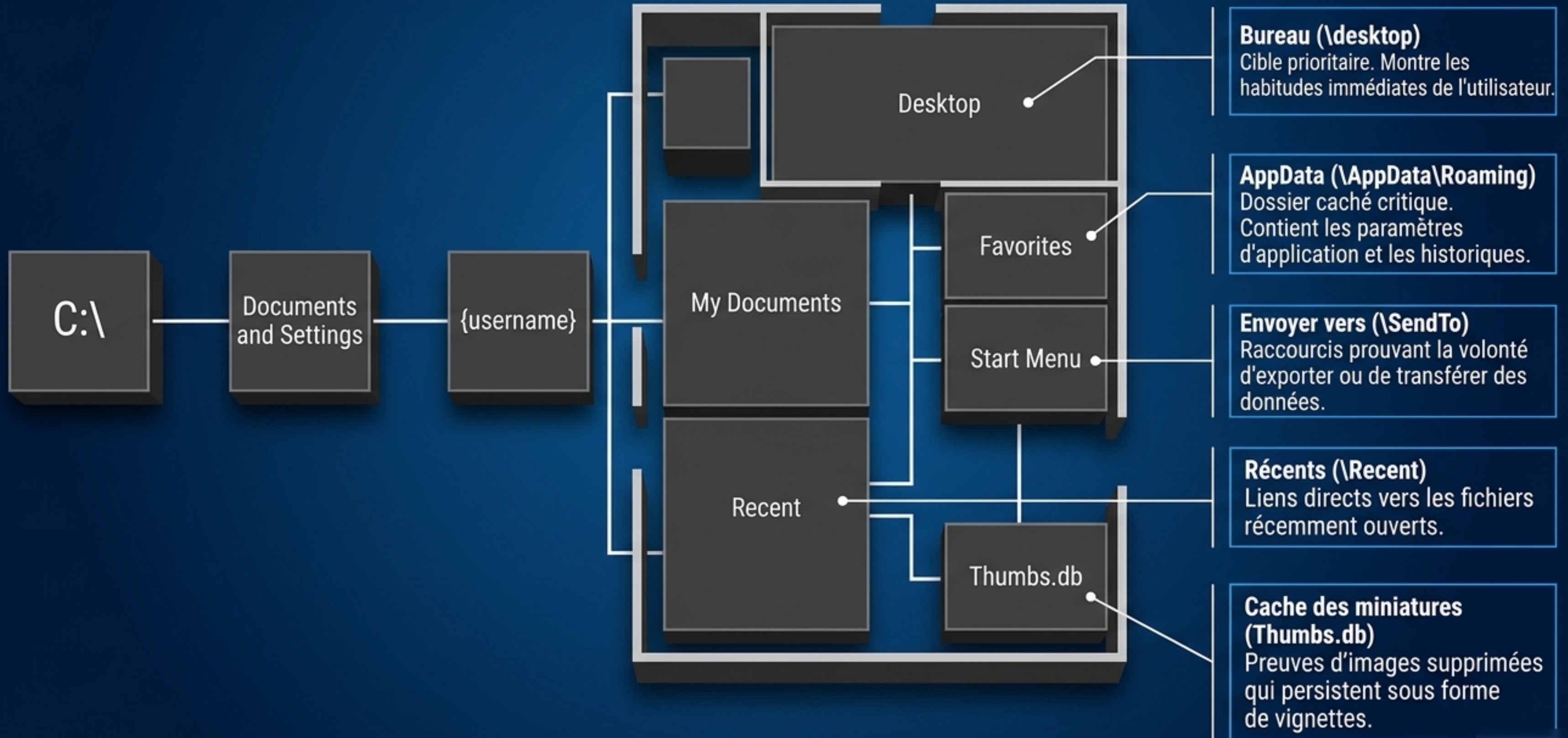
	FAT32 Héritage / Clés USB	exFAT Hybride / Amovible	NTFS Standard Entreprise
Taille max. du volume	32 Go (OS) / 2 To (Certains OS)	128 Po	2^32 clusters
Taille max. des fichiers	4 Go	16 Eo	16 To
Sécurité intégrée	Aucune	Oui (ACL minimale)	Oui
Récupérabilité	Non	Oui (si TFAT activé)	Oui

Le Paradoxe de FAT : L'absence totale de mécanismes de chiffrement et de sécurité natifs dans le système FAT est un avantage majeur pour l'analyste forensique, facilitant l'investigation directe.

Le Registre Windows : Le Cerveau du Système



Cartographie Spatiale du Profil Utilisateur



Preuves Involontaires : Prouver l'Intention

Deux artefacts souvent négligés mais dévastateurs en cour.

Les Raccourcis (.LNK)



- Présents sur le bureau ou dans les applications récentes.
- Prouve la connaissance et l'organisation volontaire d'un fichier.
- Réfute l'allégation de « téléchargement accidentel ».
- Les métadonnées révèlent la date et l'heure d'utilisation.

Fichiers Spouleurs d'Impression (.SPL / .SHD)

Name	Date modified	Type
FP00266.SHD	4/10/2013 3:29 AM	SHD File
FP00266.SPL	4/1/2013 8:27 AM	SPL File
FP00291.SHD	4/2/2013 11:22 PM	SHD File
FP00291.SPL	4/2/2013 8:08 AM	SPL File
FP00455.SHD	4/17/2013 7:43 AM	SHD File
FP00455.SPL	4/17/2013 7:43 AM	SPL File
FP00455.SHD	4/17/2013 7:43 AM	SHD File
FP00455.SPL	4/17/2013 7:43 AM	SPL File

- Générés lors d'une tentative d'impression.
- Le fichier fantôme (.shd) trace l'intention d'imprimer.
- Le mode EMF encapsule un en-tête unique identifiant l'OS d'origine.
- Prouve l'exportation physique volontaire de données.

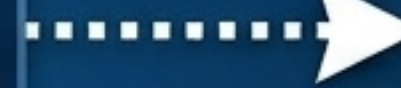
Le Cycle de Vie d'une Suppression

Systeme FAT

Fichier supprimé



Le 1^{er} caractère du répertoire est remplacé par 0xE5 (Hex).



L'index est conservé, les données restent sur le disque.

L'Illusion de l'Effacement : L'espace est libéré pour le système, mais les données physiques restent intactes sur les plateaux magnétiques jusqu'à ce qu'elles soient écrasées par de nouvelles écritures.

Systeme NTFS

Fichier supprimé



L'indicateur IN_USE est effacé dans la MFT.



Les clusters sont marqués « non alloués ».

Exception : La Menace SSD

La fonction TRIM des disques SSD formate automatiquement les blocs inutilisés, détruisant définitivement les données.

Décoder la Corbeille Windows



00000	49	4E	44	58	28	00	09	00-45	F4	68	E0	10	00	00	00	INDX(..Eôhà...
00010	00	00	00	00	00	00	00	00-28	00	00	00	F0	01	00	00	(..đ..
00020	E8	0F	00	00	00	00	00	00-20	00	00	00	00	00	00	00	è.....
00030	00	00	CF	01	70	00	00	00-00	00	00	00	00	00	00	00	..İ.p.....
00040	2C	5C	02	00	00	00	53	00-70	00	5A	00	00	00	00	00	,...S.p.Z.....
00050	7A	02	00	00	00	00	02	00-73	DC	62	72	1A	2E	D1	01	z.....sÜbr...
00060	73	DC	62	72	1A	2E	D1	01-73	DC	62	72	1A	2E	D1	01	sÜbr...sÜbr...
00070	73	DC	62	72	1A	2E	D1	01-20	02	00	00	00	00	00	00	sÜbr....

Le Décodage du Fichier \$I révèle :

- Le nom d'origine
- La taille exacte
- La date et l'heure de suppression
- Le chemin d'accès complet

L'Identificateur (SID) : La corbeille crée des sous-dossiers (ex: S-1-5-...-1007) permettant d'associer mathématiquement une suppression à un utilisateur précis.

L'Art de la Récupération de Données

```
foremost -t all -v -i /dev/sdb1 -o /root/Desktop/recover/
```

Récupérer tous les types de fichiers identifiables.

L'image disque source (ex: clé USB).

Dossier de destination sécurisé pour la preuve.

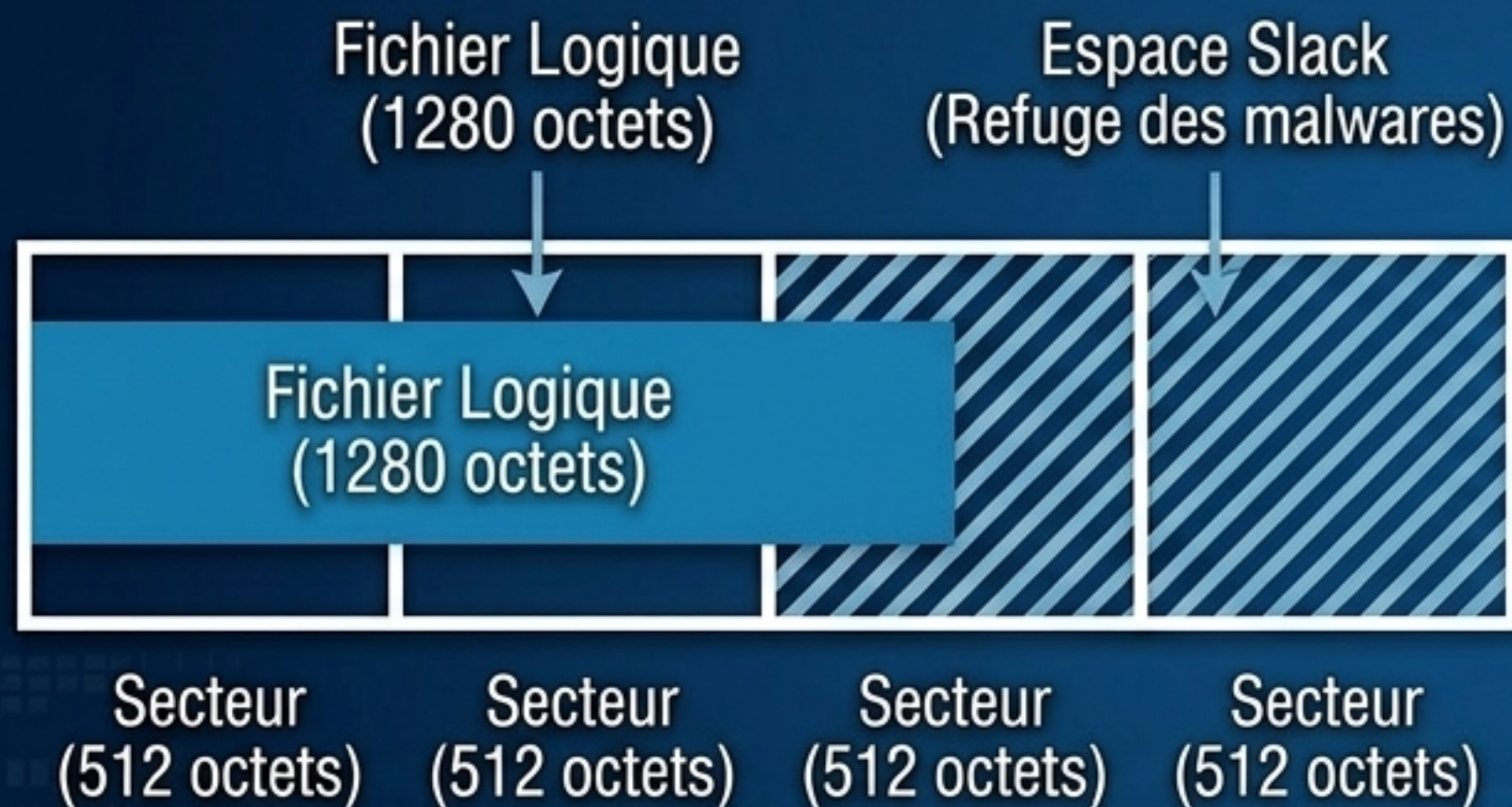
Architecture de Sortie

Foremost recrée des dossiers isolés par type de fichier (JPG, PDF, DOCX), ce qui facilite le tri massif des données récupérées.

Note Stratégique : Privilégier les outils Open Source permet à l'expert de comprendre et de justifier les mécanismes profonds de l'extraction en cour.

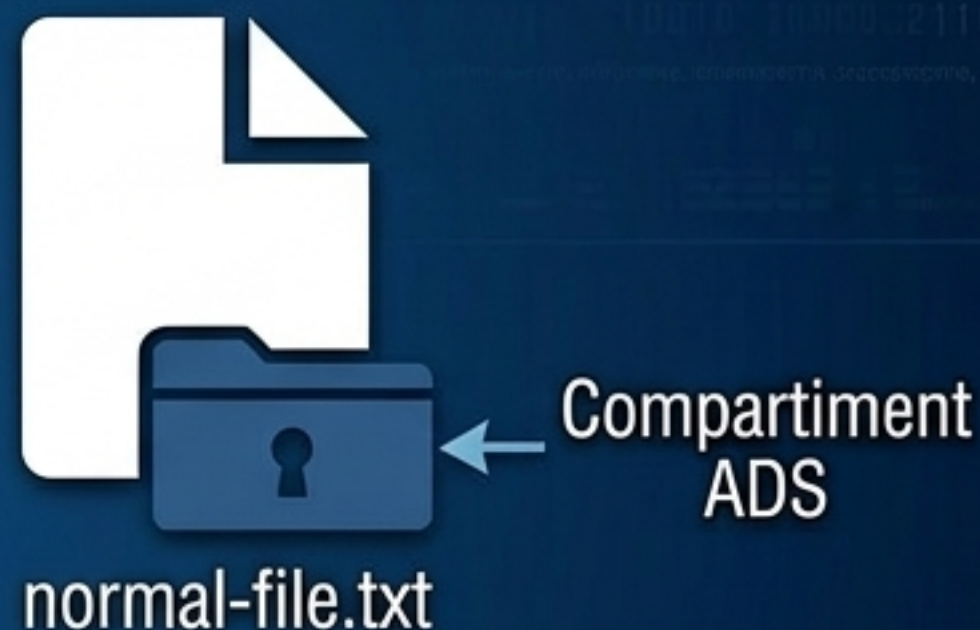
Les Zones d'Ombre : Espace Slack et ADS

L'Espace Slack (Espace Inutilisé)



La différence entre la taille logique du fichier et l'espace physique alloué par le système. Invisible pour l'OS, exploitable par un attaquant.

Flux de Données Alternatifs (ADS)



```
echo "Ceci est un code malveillant"  
> normal-file.txt:ads.txt
```

Sous NTFS, l'ADS permet de cacher des données ou des exécutables derrière un fichier légitime, sans en modifier la taille apparente ou l'extension.

L'Alternative : L'Écosystème macOS



L'Héritage (NeXTSTEP / UNIX)

Le socle BSD (noyau Mach) apportant une stabilité structurelle historique.



L'Ère Classique (HFS+)

1998 - 2017. Le système dominant pendant deux décennies. Encore très présent sur le matériel d'ancienne génération.



Le Nouveau Paradigme (APFS)

Depuis 2017.
Le standard actuel d'Apple.



L'Impact Forensique d'APFS :

APFS modifie radicalement les règles de l'acquisition. L'optimisation agressive pour SSD, les instantanés du système, et surtout le chiffrement natif, complexifient drastiquement l'analyse brute des images disques.

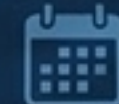
Le Radar macOS : Les Fichiers Plist

Les fichiers .plist (Property List) sont l'équivalent conceptuel du Registre Windows pour stocker les préférences et configurations.



Version du Système

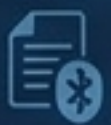
`/System/Library/CoreServices/SystemVersion.plist`



Date d'Installation Originelle

`/var/db/.AppleSetupDone`

La date de création de ce fichier caché équivaut à la naissance du système.



Historique des Périphériques

`/Bibliothèque/Préférences/com.apple.Bluetooth.plist`

Trace de toutes les connexions sans fil et périphériques externes.



Préférences Utilisateur & Réseau

`/Utilisateurs/<nom>/Bibliothèque/Préférences/*.plist`

`.../SystemConfiguration/com.apple.smb.server.plist`

Synthèse : La Matrice de l'Enquêteur

Relier l'objectif de l'investigation aux artefacts numériques à vérifier.

		Artefacts & Localisations			
Objectifs de l'Enquête		Raccourcis & Corbeille	Ruches Registre (Run / USB)	Fichiers Spool (.SPL/.SHD)	Espace Slack / ADS
1.	Prouver l'Organisation / L'Intentionnalité				
2.	Identifier la Source d'une Infection				
3.	Retracer l'Exfiltration de Données				
4.	Excaver le Contenu Détruit				

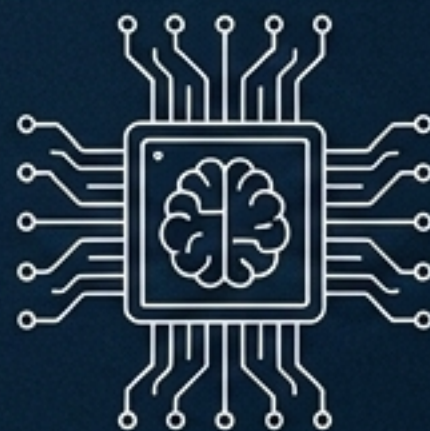
« La clé de l'investigation numérique
n'est pas de maîtriser l'outil, mais de savoir
exactement où chercher. »



1

La Surface

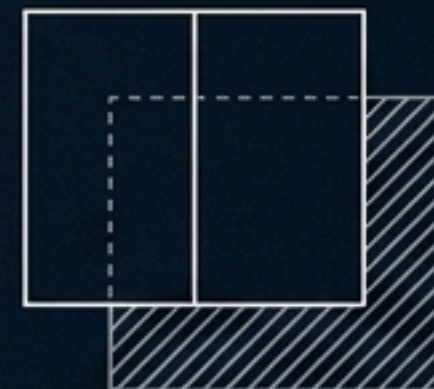
Les Métadonnées,
Exiftool, Raccourcis.



2

Le Système

Registre Windows,
Fichiers Plist, Hives.



3

Les Ombres

Espace Slack,
Fichiers \$I/\$R, Flux ADS.